ICS-CERT
INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

ICS-CERT ADVISORY

ICSA-13-067-02—INVENSYS WONDERWARE WIN-XML EXPORTER IMPROPER INPUT VALIDATION VULNERABILITY

March 21, 2013

OVERVIEW

This advisory was originally posted to the US-CERT secure Portal library on March 08, 2013, and is now being released to the ICS-CERT Web page.

This advisory provides mitigation details for a vulnerability that impacts the Invensys Wonderware Win-XML Exporter.

Researchers Timur Yunusov, Alexey Osipov, and Ilya Karpov of the Positive Technologies Research Team have discovered an improper input validation vulnerability in the Invensys Wonderware Win-XML Exporter. Invensys has released a patch that mitigates the vulnerability. The Positive Technologies Research Team has validated that the patch fixes the vulnerability. Exploitation of this vulnerability could impact systems deployed in the critical manufacturing, energy, food and beverage, chemical, and water and wastewater sectors.

AFFECTED PRODUCTS

The following Invensys Wonderware products are affected:

- Win-XML Exporter Version 1522, 148, 0, 0, and possibly earlier versions.

IMPACT

Successful exploitation of this vulnerability could allow an attacker to affect the confidentiality and availability of the Wonderware Win-XML Exporter.

ICS-CERT
INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

Impact to individual organizations depends on many factors that are unique to each organization. ICS-CERT recommends that organizations evaluate the impact of this vulnerability based on their operational environment, architecture, and product implementation.

BACKGROUND

Invensys is a global technology company that works with industrial, commercial, rail operators, and appliance operators, while operating in over 180 countries. Invensys develops software, systems, and equipment that enable users to monitor, automate, and control their processes.

The Invensys[a] Wonderware Win-XML Exporter is used in many industries worldwide, including critical manufacturing, energy, food and beverage, chemical, and water and wastewater.

The Wonderware Win-XML Exporter converts interface windows from Intouch HMI projects and displays them in Internet Explorer with the help of Wonderware Information Server.

VULNERABILITY CHARACTERIZATION

VULNERABILITY OVERVIEW

IMPROPER INPUT VALIDATION[b]

Wonderware Win-XML Exporter allows access to local resources (files and internal resources) via unsafe parsing of XML external entities. By using specially crafted XML files, an attacker can cause Wonderware Win-XML Exporter to send the contents of local or remote resources to the attacker's server or cause a denial of service of the system.

CVE-2012-4710[c] has been assigned to this vulnerability. A CVSS v2 base score of 6.3 has been assigned; the CVSS vector string is (AV:L/AC:M/Au:N/C:C/I:N/A:C).[d]

a. http://www.invensys.com/, Web site last accessed March 21, 2013.

b. CWE-20 Improper Input Validation, http://cwe.mitre.org/data/definitions/20.html, Web site last accessed March 21, 2013.

c. NVD, http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-4710, NIST uses this advisory to create the CVE Web site report. This Web site will be active sometime after publication of this advisory.

d. CVSS Calculator, http://nvd.nist.gov/cvss.cfm?version=2&vector=(AV:L/AC:M/Au:N/C:C/I:N/A:C), Web site last visited March 21, 2013.

ICS-CERT
INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

VULNERABILITY DETAILS

EXPLOITABILITY

This vulnerability is not exploitable remotely and cannot be exploited without user interaction. The exploit is only triggered when a local user runs the vulnerable application and loads the malformed XML files.

EXISTENCE OF EXPLOIT

No known public exploits specifically target this vulnerability.

DIFFICULTY

An attacker with a medium skill would be able to exploit this vulnerability.

MITIGATION

Invensys has developed an update to the Win-XML Exporter that mitigates this vulnerability. The Positive Technologies Research Team has tested the update and validated that it fixes the vulnerability. Instructions and a link to the update are found on the Invensys download page.[e]

According to Invensys, any machine running one or more of the products listed above is affected and should be patched. No other components of the Wonderware installed products are affected. Users should install the update using instructions provided in the ReadMe file for the product and component being installed. Invensys recommends that users:

- Read the installation instructions provided with the patch.
- Shut down any of the affected software products.
- Install the update.
- Restart the software.

ICS-CERT encourages asset owners to take additional defensive measures to protect against this and other cybersecurity risks.

- Minimize network exposure for all control system devices. Critical devices should not directly face the Internet.

e. Invensys software download page, https://wdn.wonderware.com/sites/WDN/Pages/Downloads/Software.aspx, Web site last accessed March 21, 2013.

- Locate control system networks and remote devices behind firewalls, and isolate them from the business network.
- When remote access is required, use secure methods, such as Virtual Private Networks (VPNs), recognizing that VPN is only as secure as the connected devices.

ICS-CERT also provides a section for control systems security recommended practices on the ICS-CERT Web page. Several recommended practices are available for reading and download, including Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies.[f] ICS-CERT reminds organizations to perform proper impact analysis and risk assessment prior to taking defensive measures.

Additional mitigation guidance and recommended practices are publicly available in the ICS-CERT Technical Information Paper, ICS-TIP-12-146-01B—Targeted Cyber Intrusion Detection and Mitigation Strategies,[g] that is available for download from the ICS-CERT Web page (www.ics-cert.org).

Organizations observing any suspected malicious activity should follow their established internal procedures and report their findings to ICS-CERT for tracking and correlation against other incidents.

ICS-CERT CONTACT

For any questions related to this report, please contact ICS-CERT at:

Email: ics-cert@hq.dhs.gov
Toll Free: 1-877-776-7585
For industrial control systems security information and incident reporting: www.ics-cert.org

ICS-CERT continuously strives to improve its products and services. You can help by answering a short series of questions about this product at the following URL: https://forms.us-cert.gov/ncsd-feedback/.

f. CSSP Recommended Practices, http://www.us-cert.gov/control_systems/practices/Recommended_Practices.html, Web site last accessed March 21, 2013.

g. Targeted Cyber Intrusion Detection and Mitigation Strategies, http://www.us-cert.gov/control_systems/pdf/ICS-TIP-12-146-01B.pdf, Web site last accessed March 21, 2013.

ICS-CERT
INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

DOCUMENT FAQ

What is an ICS-CERT Advisory? An ICS-CERT Advisory is intended to provide awareness or solicit feedback from critical infrastructure owners and operators concerning ongoing cyber events or activity with the potential to impact critical infrastructure computing networks.

When is vulnerability attribution provided to researchers? Attribution for vulnerability discovery is always provided to the vulnerability reporter unless the reporter notifies ICS-CERT that they wish to remain anonymous. ICS-CERT encourages researchers to coordinate vulnerability details before public release. The public release of vulnerability details prior to the development of proper mitigations may put industrial control systems and the public at avoidable risk.

I see that this document is labeled as TLP = WHITE. May I distribute this to other people? According to the International Critical Information Infrastructure Protection (CIIP) Traffic Light Protocol[h,i] warning, this document is subject to standard copyright rule and may be distributed freely without restriction.

TLP = WHITE: Unlimited

h. Traffic Light Protocol—International CIIP Directory, Issue 21, September 2009.
i. US-CERT, http://www.us-cert.gov/tlp/, Web site last accessed March 05, 2013.